

REMARKS

In view of the following remarks, Applicants respectfully request reconsideration and allowance of the subject application. Claims 6 and 7 are canceled without prejudice, Claims 8 and 9 are as originally filed, Claims 2-5, 10 and 16 were previously presented, and Claims 1, 11-15 and 17-21 are currently amended. Accordingly, Claims 1-5 and 8-21 are pending.

Claim Objections

Claim 14 is objected to because of an informality noted by the Examiner. Applicants have amended Claim 14 to make the noted correction.

Claim Rejection under 35 U.S.C. § 112

Claim 18 is rejected under 35 U.S.C 112 because there is insufficient antecedent basis for the limitation of “the first value” and “the threshold.” Applicants have amended Claim 18 to correct the antecedent basis of the noted limitations.

Claim Rejection under 35 U.S.C. § 101

Claims 1-5 and 8-21 are rejected under 35 U.S.C 101 because the claims are non-tangible or are not limited to tangible embodiments. Applicants have amended Claims 1, 11-15 and 17-21 to limit the scope of the claims to tangible embodiments.

Claim Rejection under 35 U.S.C. § 102

Claims 1-5, 8-17 and 19-21 stand rejected under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 6,463,535 to Drews. Applicants respectfully traverse the rejection of Claims 1-5, 8-17 and 19-21. Drews discloses a technique for downloading a boot image to a local platform. The technique utilizes a signed manifest 150 transmitted with the boot image and an authorization certificate 280 stored on the local platform to verify the integrity of the downloaded boot image. The signed manifest 150 is also utilized to confirm that the boot image was received from an authorized source.

Claim 1, as amended, recites a method of associating a permission set with a code assembly based on evidence characterized by different levels of trust, the method implemented at least in part by a computing device that includes:

- identifying a first condition for association with the permission set, wherein the first condition references a first element of evidence, wherein the first element of evidence is implicitly trusted and wherein the permission set is used to control operation of the code assembly during run-time;
- identifying a second condition for association with the permission set, wherein the second condition references a second element of evidence, wherein the second element of evidence is initially untrusted;
- determining whether the first condition is satisfied by the first element of evidence;

- determining whether the second element of evidence should be trusted based on the first condition;
- determining whether the second condition is satisfied by the second element of evidence; and
- associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.

Drews does not disclose “identifying a first condition for association with the permission set ... wherein the permission set is used to control operation of the code assembly during run-time” or “identifying a second condition for association with the permission set.” Applicants cannot find any mention of a “permission set” in Drews. Furthermore, the Office has failed to identify what element in Drews is equivalent to “a permission set,” and in particular a “permission set” that is “used to control operation of the code assembly during run-time.”

Furthermore, Drews does not disclose “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.” Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing

the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not include “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied” wherein “the permission set is used to control operation of the code assembly during run-time.” For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew only discloses determining if an application is authorized to run and not associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 1 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 1 be withdrawn and that Claim 1 be allowed.

Claims 2-5 and 8-10 are allowable by virtue of their dependency on respective base Claim 1, as well as the additional elements they recite. Accordingly, Applicants respectfully request that the §102 rejection of Claims 2-5 and 8-10 be withdrawn and that Claims 2-5 and 8-10 be allowed.

Claim 11, as amended, recites one or more computer-readable media having instructions that, when executed on one or more processors perform a process for

associating a permission set with a code assembly based on evidence characterized by different levels of trust that includes:

- generating a collection of code groups, wherein each code group is used to define a category of related code assemblies, each code group being associated with a membership criterion and a permission set used to control operation of the code assembly during run-time;
- receiving the membership criterion associated with one of the code groups, the membership criterion including at least a first condition and a second condition;
- referencing a first element of evidence in the first condition, wherein the first element of evidence is trusted independent of other evidence and conditions;
- referencing a second element of evidence in the second condition, wherein the second element of evidence is initially untrusted;
- determining whether the first condition is satisfied by the first element of evidence;
- determining whether the second element of evidence should be trusted based on the first condition;
- determining whether the second condition is satisfied by the second element of evidence;

- evaluating the first condition and the second condition using a logical operation to determine membership of the code assembly in the code group; and
- associating the permission set with the code assembly, if the code assembly is determined to be a member of the code group.

The Office asserts that Claim 11 is rejected for the same reasons advanced in support of Claim 1-5 and 8-10. However, Applicants respectfully submit that Drews does not disclose “generating a collection of code groups, wherein each code group is used to define a category of related code assemblies.” Applicants cannot find any mention of a “code group” in Drews, and in particular “a code group used to define a category of related code assemblies.” Furthermore, the Office has failed to identify what element in Drews is equivalent to a “code group” or how a “code group” is inherent in any element discussed in Drews. In addition, Drews does not disclose “each code group being associated with a membership criterion and a permission set used to control operation of the code assembly during run-time.” Applicants cannot find any mention of a “permission set” in Drews, and in particular “a permission set used to control operation of the code assembly during run-time.”

Applicants also respectfully submit that Drews does not disclose “evaluating the first condition and the second condition using a logical operation to determine membership of the code assembly in the code group.” Applicants cannot find any mention of determining “membership” of “a code assembly.” Furthermore, the Office

has failed to identify what element in Drews is equivalent to “determining membership of the code assembly in the code group” or how it is inherent in any element discussed in Drews. Instead, the passage relied upon by the Office, col. 4, lines 1-14, generally describes a verification function that determines the integrity of the downloaded boot image and whether the boot image has been provided by an acceptable source.

Furthermore, Drews does not disclose “associating the permission set with the code assembly, if the code assembly is determined to be a member of the code group.” Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not disclose “associating the permission set with the code assembly, if the code assembly is determined to be a member of the code group” wherein “the permission set is used to control operation of the code assembly during run-time.” For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can

affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew only discloses determining if an application is authorized to run and not associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 11 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 11 be withdrawn and that Claim 11 be allowed.

Claim 12 is allowable by virtue of its dependency on respective base Claim 11, as well as the additional elements it recites. Accordingly, Applicants also request that the §102 rejection of Claim 12 be withdrawn and that Claim 12 be allowed.

Claim 13, as amended, recites one or more computer-readable media having computer-executable instructions for performing a method of associating a permission set with a code assembly based on evidence characterized by different levels of trust that includes:

- receiving a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set and the first element of evidence is trusted independent of other evidence and conditions;
- receiving a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set and the second element is initially untrusted;

- determining whether the first condition is satisfied by the first element of evidence;
- determining whether the second element should be trusted based on the first condition;
- determining whether the second condition is satisfied by the second element of evidence; and
- associating the permission set with the code assembly, if both the first and second conditions are satisfied, **wherein the permission set is used to control operation of the code assembly during run-time.**

Drews does not disclose “identifying a first condition for association with the permission set” or “identifying a second condition for association with the permission set.” Applicants cannot find any mention of a “permission set” in Drews. Furthermore, the Office has failed to identify what element in Drews is equivalent to “a permission set,” or how “a permission set” is inherent in any element discussed in Drews.

Furthermore, Drews does not disclose “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied, wherein the permission set is used to control operation of the code assembly during run-time.” Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the

boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not include “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied” wherein “the permission set is used to control operation of the code assembly during run-time.” For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew only discloses determining if an application is authorized to run and not associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 13 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 13 be withdrawn and that Claim 13 be allowed.

Claim 14, as amended, recites one or more computer-readable media having instructions that, when executed on one or more computing processors, perform a process for associating a permission set with a code assembly based on evidence characterized by different levels of trust that includes:

- receiving at least a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set and the first element of evidence is trusted independent of other evidence and conditions;
- receiving at least a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set and the second element is initially untrusted;
- determining whether the first condition is satisfied by the first element of evidence;
- determining whether the second element of evidence should be trusted based on the first condition;
- determining whether the second condition is satisfied by the second element of evidence; and
- associating the permission set with the code assembly, if both the first and second conditions are satisfied, wherein the permission set is used to control operation of the code assembly during run-time.

Drews does not disclose “receiving at least a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set” or “receiving at least a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set.” Applicants cannot find any mention of a “permission set” in Drews. Furthermore, the Office has

failed to identify what element in Drews is equivalent to “a permission set,” or how “a permission set” is inherent in any element discussed in Drews.

Furthermore, Drews does not disclose “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied, wherein the permission set is used to control operation of the code assembly during run-time.” Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not include “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied” wherein “the permission set is used to control operation of the code assembly during run-time.” For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew

only discloses determining if an application is authorized to run and not associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 14 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 14 be withdrawn and that Claim 14 be allowed.

Claim 15, as amended, recites a policy manager for associating a permission set with a code assembly based on evidence characterized by different levels of trust that includes:

- a code collection generator generating a collection of code groups, **wherein each code group is used to define a category of related code assemblies**, each code group being associated with the membership criterion and a **permission set used to control operation of the code assembly during run-time;**
- a membership evaluator determining if the code assembly is a member of the code group by evaluating at least a first condition and a second condition associated with one of the code groups, the first condition referencing an implicitly trusted first element of evidence; the second condition referencing an initially untrusted second element of evidence, wherein a determination of trust associated with the second element of evidence is based on the first condition; and

- a permission set generator associating the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group.

Drews does not disclose “a code collection generator generating a collection of code groups, wherein each code group is used to define a category of related code assemblies.” Applicants cannot find any mention of a “code group” in Drews, and in particular “a code group used to define a category of related code assemblies.” Furthermore, the Office has failed to identify what element in Drews is equivalent to a “code group” or how a “code group” is inherent in any element discussed in Drews. In addition, Drews does not disclose “each code group being associated with a membership criterion and a permission set used to control operation of the code assembly during run-time.” Applicants cannot find any mention of a “permission set” in Drews, and in particular “a permission set used to control operation of the code assembly during run-time.”

Applicants also respectfully submit that Drews does not disclose “a membership evaluator determining if the code assembly is a member of the code group by evaluating at least a first condition and a second condition associated with one of the code groups.” Applicants cannot find any mention of “determining if the code assembly is a member of a code group.” Furthermore, the Office has failed to identify what element in Drews is equivalent to “determining if the code assembly is a member of a code group” or how it is inherent in any element discussed in Drews.

Instead, the passage relied upon by the Office, col. 4, lines 1-14, generally describes a verification function that determines the integrity of the downloaded boot image and whether the boot image has been provided by an acceptable source.

Furthermore, Drews does not disclose “a permission set generator associating the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group.” Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not disclose “associating the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group” wherein “the permission set is used to control operation of the code assembly during run-time.” For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew only discloses determining if an application is authorized to run and not

associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 15 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 15 be withdrawn and that Claim 15 be allowed.

Claim 16 is allowable by virtue of its dependency on respective base Claim 15, as well as the additional elements it recites. Accordingly, Applicants also request that the §102 rejection of Claim 16 be withdrawn and that Claim 16 be allowed.

Claim 17 , as amended, recites one or more computer-readable media having instructions that, when executed on one or more processors, perform a process for associating a permission set with a code assembly based on evidence characterized by different levels of trust that includes:

- receiving one or more first conditions, each first condition being associated with one or more first elements of evidence, wherein each first condition is associated with the permission set used to control operation of the code assembly during run-time;
- determining whether each first condition is satisfied by an associated first element of evidence;
- generating an indication for each first condition that is satisfied;
- receiving a second condition associated with the permission set;
- determining whether the second condition is satisfied based on the indications, wherein a level of trust associated with the indications depends upon a first condition of the one or more first conditions; and
- associating the permission set with the code assembly, if both the first condition in the second condition are satisfied.

Drews does not disclose “receiving one or more first conditions ... wherein each first condition is associated with the permission set used to control operation of the code assembly during run-time,” or “receiving a second condition associated with the permission set.” Applicants cannot find any mention of a “permission set” in Drews. Furthermore, the Office has failed to identify what element in Drews is equivalent to “a permission set,” and in particular a “permission set” that is “used to control operation of the code assembly during run-time.” Consequently, Applicants

also respectfully assert that Drews does not disclose that a “permission set” is associated with “each first condition” and “a second condition”

Furthermore, Drews does not disclose “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.” Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not include “associating the permission set with the code assembly, if both the first condition and the second condition are satisfied” wherein “the permission set is used to control operation of the code assembly during run-time.” For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew only discloses determining if an application is authorized to run and not associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 17 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 17 be withdrawn and that Claim 17 be allowed.

Claims 19-21 are allowable by virtue of their dependency on respective base Claim 17, as well as the additional elements they recite. Accordingly, Applicants respectfully request that the §102 rejection of Claims 19-21 be withdrawn and that Claims 19-21 be allowed.

Claim Rejection under 35 U.S.C. § 103

Claim 18 stands rejected under 35 U.S.C. § 103 as being obvious in view of the combination of U.S. Patent No. 6,463,535 to Drews and U.S. Patent No. 6,687,823 to Al-Salqan. Applicants respectfully submit that Al-Salqan does not cure the defects of Drews that were previously described. Accordingly, Claim 18 is allowable over the combination of Drews and Al-Salqan for at least the reasons discussed above with regard to Claim 17. Applicants therefore request that the §103 rejection of Claim 18 be withdrawn and that Claim 18 be allowed.

Conclusion

Claims 1-5 and 8-21 are believed to be in condition for allowance. Applicant respectfully requests prompt allowance of the subject application. Should any issue

remain unresolved that would prevent allowance of this case, the Examiner is requested to contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Date: 1/30/06

By: 
1/30/06

Eric J. Gash
Lee & Hayes, PLLC
Reg. No. 46,274
(509) 324-9256 ext. 228